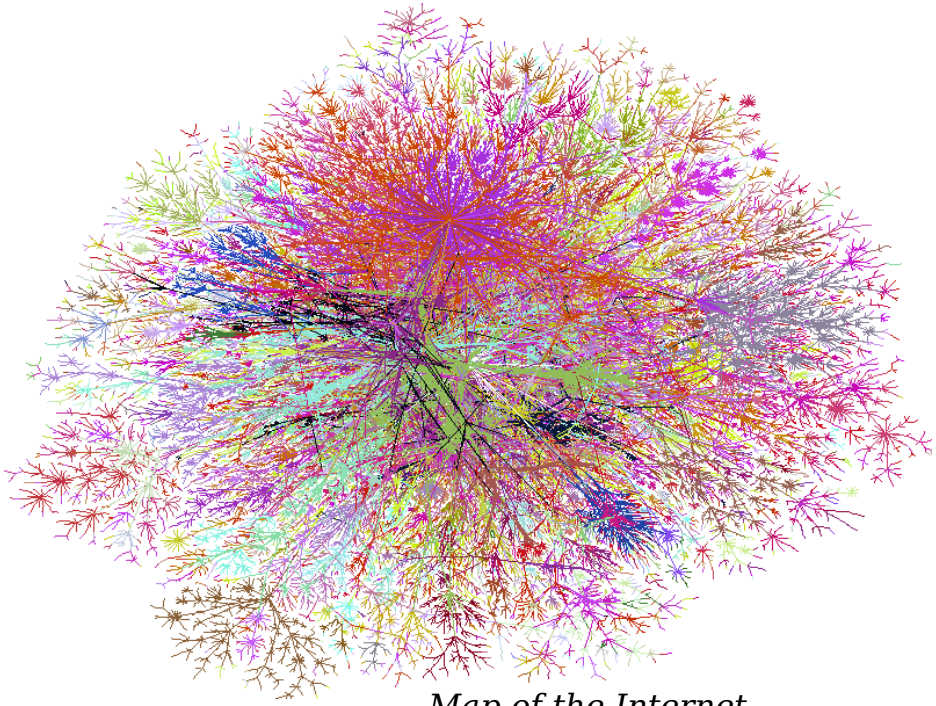
Risk Management for Opaque Networks

"Hitting the Moving Target"

De Ann Pope

Enterprises are no longer self-contained!

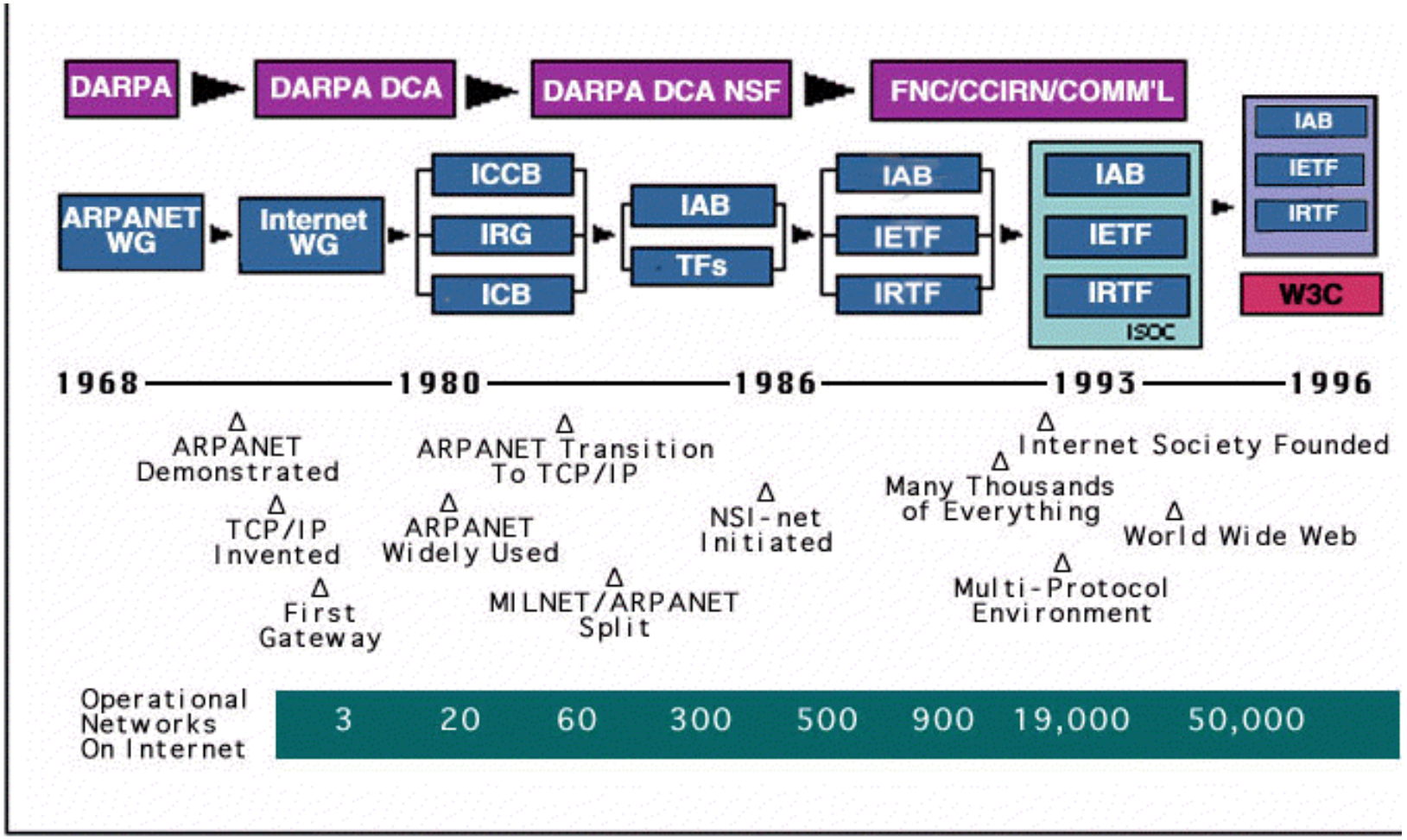
"From the edge of a corporate network to the user desktop, you can no longer control the flow of information ."



Map of the Internet

December 1998 – Wired Magazine

History of the Network



History of the Network

Client/Server Applications

Applications on closed networks

Networks + gateway for occasional email & web-browsing

Networks using the Internet for site-to-site communications, email, web-browsing, collaboration, etc.

Threats

Trojans
Tracking Cookies
Adware
Spyware
KeyLoggers
Parasites
Malware
Browser Hijacker

The Problem

- You can't ***secure*** what you can't ***manage***
- You can't ***manage*** what you can't ***define***

Do you know your true network perimeter?

Evaluating the Risk

Do you have systems, networks or applications:

1. that connect to external networks?

RISK

2. provide Internet access for users?

RISK

3. collaborate with external users?

RISK

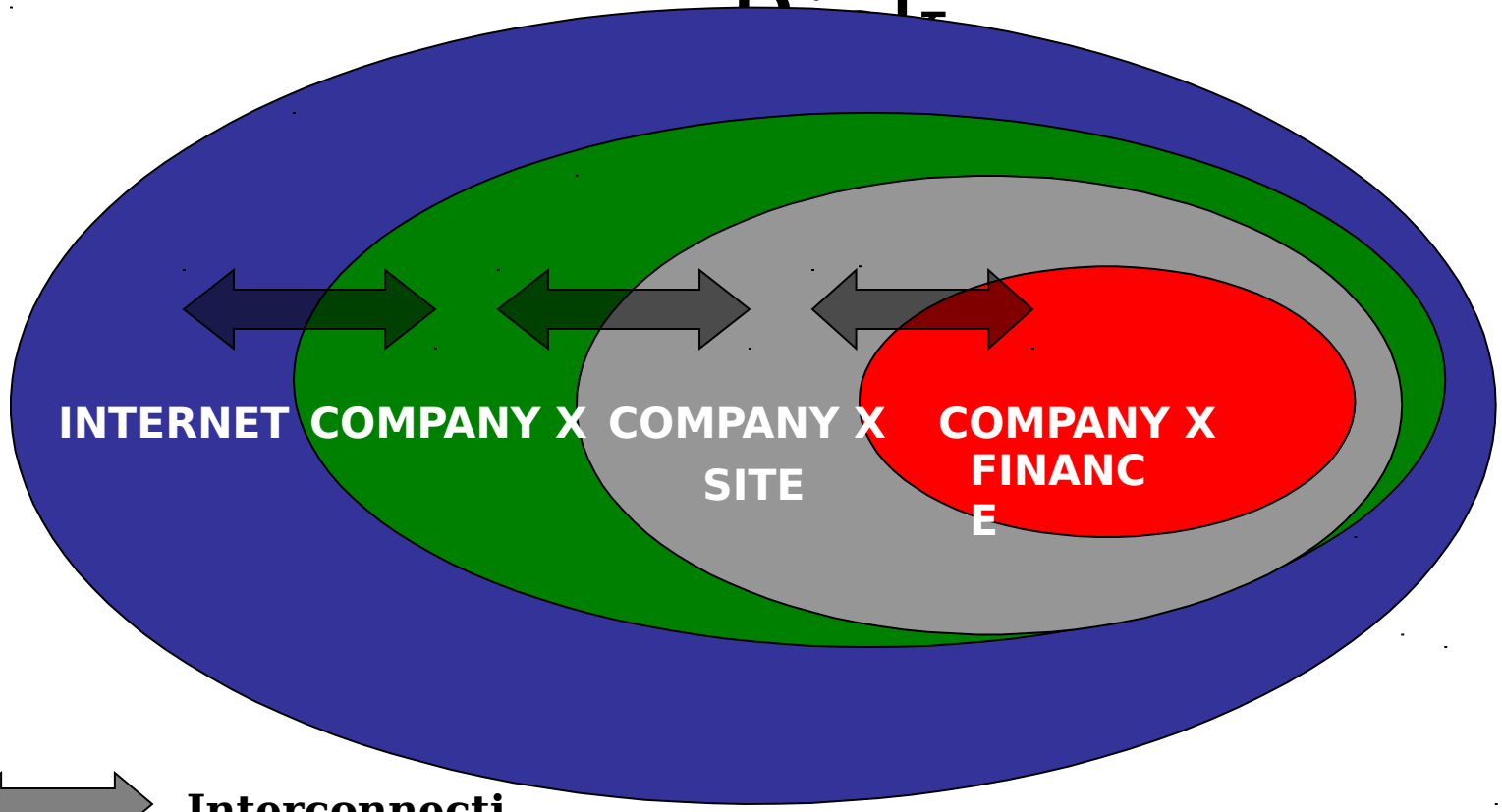
4. control all flow of data to and from your users?

RISK

Need to Change

- An approach that reduces overall risk with attainable goals
- Change the way we design and implement information security infrastructure
- Combine best of breed techniques & technologies that provide dynamic security solutions

Managing Risk



Interconnection

Define Security Domains and policies that apply when passing information through each domain.

Managing Risk

- **Focus resources at the perimeter of the network**
  - Use sound methods for access/authentication/non-repudiation & audit
  - Restrict access to suspect sites
  - Monitor port activity
  - Use VPNs & other methods for protecting communications

    Remember that email messages are digital postcards

- **Store user data on shared resources not on workstations or co-located lans (use layers of abstraction)**
  - Use multi-trackware detection and removal utilities to protect clients as much as possible.

- **Use proxy devices to control communications**

Closing Point

Managing 'interconnections' is the crux to effectively managing the perimeter of a network, providing an effective risk mitigation strategy for opaque networks.

To manage the risk, create clearly defined policies and train users to follow them!!

Thank You.

De Ann Pope
Technical Director